Declaração de Segurança Cibernética Banco BOCOM BBM

Esta Declaração de Segurança Cibernética visa oferecer ao Público (Clientes, Colaboradores, Parceiros e Fornecedores, atuais e futuros) um resumo dos princípios e ações adotadas pelo Banco BOCOM BBM para assegurar o controle e a segurança dos ativos de Informação sob sua custódia em decorrência do exercício das atividades operacionais.

Ela informa, em linhas gerais, o direcionamento e a disposição do Banco BOCOM BBM em estabelecer diretrizes e procedimentos relacionados à Segurança Cibernética, adotando um programa de implementação de políticas e procedimentos para proteger esse ambiente de vários tipos de ameaças, garantindo a Confidencialidade, Integridade e Disponibilidade das Informações, dos Sistemas e Processos de Negócios, em conformidade com exigências regulatórias (ex. Resolução Nº 4.658 do BACEN) e com as boas práticas de mercado: padrão de segurança da International Organization for Standardization **ISO 27000** e recomendações do **NIST** – National Institute of Standards and Technology.

Segurança Cibernética

O Banco BOCOM BBM se dispõe a manter em sua estrutura corporativa a Função e as atividades voltadas para a governança da Segurança Cibernética, apoiada por processos e ferramentas tecnológicas. Essa função conta com os seguintes instrumentos:

- Comitê de Segurança da Informação - CSI, cuja composição e atuação visa supervisão e assessoria na implementação das ações de Segurança Cibernética no Banco BOCOM BBM e também a constante supervisão de violações de princípios e diretrizes estabelecidas nas Políticas, Normas e Procedimentos relacionados, bem como pelo direcionamento e acompanhamento das ações e incidentes de segurança, e a aprovação de situações não previstas na presente política, possuindo a alçada necessária para tal;
- Equipes de Segurança da Informação e Segurança da Tecnologia da Informação;
- Políticas de Segurança Cibernética e de Segurança da Informação – aprovada e suportada irrestritamente pelo Conselho de Administração do BOCOM BBM e com abrangência Corporativa;
- Normas e Procedimentos relativos aos domínios de Segurança da Informação, contendo diretrizes e instruções sobre:
  - Classificação das Informações conforme sua sensibilidade;
  - Gestão de acesso lógico aos sistemas, aplicações e infraestrutura do ambiente corporativo;
  - Regras para uso dos recursos tecnológicos (computadores, redes corporativas, internet, telefonia, e-mails, armazenamentos, backups) pelos Colaboradores e Prestadores de serviços;
  - Gerenciamento de Segurança em Fornecedores contratados;
  - Direcionamentos sobre Comunicação e Tratamento de Incidentes de Segurança Cibernética;
  - Gerenciamento de alterações (mudanças) no ambiente de TI, bem como regras de desenvolvimento seguro de aplicações baseadas em Internet;
  - Planos de Contingência de Negócios;
- Revisões periódicas especializadas (Testes de Segurança e Vulnerabilidades, Auditorias independentes) buscando estabelecer o grau de efetividade das políticas, normas e procedimentos de segurança cibernética e de proteção dos ativos de informação do Banco e de seus Clientes;

- Gestão da operação de Segurança da Informação e da Segurança de Tecnologia da Informação, considerando os insumos relacionado ao ciclo de governança da segurança cibernética e correspondentes ações de Divulgação e Treinamentos sobre o tema.

Cabe ressaltar que as ações relacionadas à Segurança Cibernética são **dinâmicas**, sendo passiveis de constante monitoramento, aperfeiçoamento, revisão de aplicabilidade, abrangência e maturidade dos processos, instrumentos e ferramentas de apoio.

Glossário

A Informação é um ativo que tem alto valor para o Banco BOCOM BBM e a Segurança da Informação refere-se à proteção da mesma contra vários tipos de ameaças, sendo orientada pelos conceitos de confidencialidade, integridade, disponibilidade e Auditabilidade:

- Por Informação entende-se todo e qualquer dado, informe, relatório, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oral ou qualquer outra forma física ou eletrônica, em decorrência do desenvolvimento das atividades profissionais da instituição.
- Por Confidencialidade entende-se a garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meios eletrônicos ou físicos. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal.
- Por Integridade entende-se a fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.
- Por Disponibilidade entende-se a garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de TI. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.
- Por Ameaças entendem-se as técnicas, ferramentas, ações e/ou omissões, propositais ou não, que possibilitem contornar controles de segurança, a exploração de vulnerabilidade e consequente mau uso da Informação. Tais ameaças variam bastante, dependendo no contexto de uso da informação, mas pode-se destacar: a engenharia social, o vazamento de informações, o mau uso de credenciais de acesso, ataques cibernéticos aos sistemas e ativos de infraestrutura.
- Por Auditabilidade entende-se a garantia de que qualquer alteração, acesso, manuseio, exclusão, criação ou quaisquer outras interações relevantes com os sistemas e informação informações sejam registrados de forma adequada, íntegra e suficiente para fins de investigação e monitoração técnica e de conformidade. Manter os princípios de Auditabilidade pressupõe que os registros existam e sejam de acesso controlado e não alteráveis por usuários ou administradores do ambiente de tecnologia.